Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
NAI1P089/00.175.01	

I hereby certify that this correspondence is being e-filed with the USPTO	Application Number	Filed
on March 17, 2008	09/836,214	04/18/2001
Signature /Dana Chan/	First Named Inventor: Peter T. Dinsmore	
Typed or printed name Dana Chan	Art Unit: 2131	Examiner: Laforgia, Christian A.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KEVINZILKA/
Signature

Kevin J. Zilka
Typed or printed name

408-971-2573
Telephone number

March 17, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*

☑ *Total of 1 forms are submitted.

REMARKS

The Examiner has rejected Claims 13-15, 17-21, and 41-50 under 35 U.S.C. 102(b) as being anticipated by Balenson et al. ("Dynamic Cryptographic Context Management (DCCM): Report #1 Architecture and System Design"). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on pages 34, 47, 54, and 99 from the Balenson reference to make a prior art showing of applicant's claimed technique "wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key,...and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key" (see the same or similar, but not necessarily identical language in each of the independent claims). More specifically, the Examiner has asserted that the above reference excerpts "provid[e] a showing of the properties as backward secrecy, forward secrecy, and collusion-resistance."

Applicant respectfully points out that the Balenson reference excerpts relied upon by the Examiner merely teach that "[i]f a private key is compromised, all digital certificates containing the matching public key must be revoked" and that "[t]his is reported back to the certificate server where the on-line certificate repository is updated" (Page 34, first paragraph – emphasis added). The excerpts further teach that "[s]ecret keys have to be transmitted... in a confidential manner such that they cannot be modified or replaced by another key in an unauthorized and undetected manner" and that "[k]eys have to be... protected in a user-friendly and failsafe manner" (Page 34, fourth and fifth paragraphs – emphasis added).

Additionally, the excerpts from Balenson teach "encrypt[ing] the data," "detection mechanisms [that] serve to reduce the probability of compromise," and "[a] trust model" (Page 47, second and third paragraphs – emphasis added). Further, the excerpts disclose that "the enrollment process establishes for each member an *individual DCCM base key*

known only to the member and his enrolling DCCM manager" and that "these DCCM base keys allow for certain efficiencies in establishing individual group base keys" (Page 54, second paragraph – emphasis added), in addition to "establishing for each group member an individual group base key known only to the member and the group manager" and "repeat[ing] a pair-wise authenticated key exchange protocol separately for each group member" (Page 54, third paragraph – emphasis added).

Further still, the aforementioned excerpts teach that "in order to prevent collusion by two or more evicted members, a large amount of information must be predistributed" (Page 99, ninth paragraph -emphasis added). In particular, such excerpt from Balenson discloses that "[w]hen a member is evicted, the remaining group members can use this predistributed information to compute a new key, without any trusted controller separately transmitting the new key" (Page 99, ninth paragraph - emphasis added).

However, applicant respectfully asserts that generally disclosing revoking digital certificates with a public key if a matching private key is compromised, protecting keys and transmitting keys in a confidential manner, encrypting data, utilizing detection mechanisms and a trust model, establishing a base key known only to a member and an enrolling manager, in addition to disclosing that "a large amount of information must be predistributed," such that "remaining group members can use this predistributed information to compute a new key," as in Balenson, does not teach that "said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key," and "(3) knowledge of said first key and said updated first key does not give any knowledge of said second key," as specifically claimed by applicant.

In particular, simply disclosing the revoking of a public key if the matching private key is compromised, encrypting data and establishing a base key known only to a member and an enrolling manager, as well as the use of predistributed information to compute a new key, as in Balenson, does not suggest, and especially does not rise to the level of specificity of, applicant's claim language, namely that "knowledge of said

updated first key does not give knowledge of said first key or said second key...and...knowledge of said first key and said updated first key does not give any knowledge of said second key" (emphasis added), as claimed.

In the Office Action mailed 12/17/2007, the Examiner has cited *Texas Instruments Inc. v. U.S. International Trade Commission* and has argued that "[t]he Examiner has afforded the [aforementioned] limitation very little patentable weight since wherein clauses in method claims are not given weight when they simply express the intended result of a process step positively recited." Additionally, the Examiner has cited *Minton v. National Association of Securities Dealers, Inc.* and has argued that "[i]n this case the wherein clause merely expresses properties that result from the determining step" and that "the properties disclosed in the wherein clause do not provide any information regarding the mechanics of how the determining step is executed."

Applicant respectfully disagrees. Applicant respectfully asserts that, when taken in context, applicant claims that "said determining [an updated first key] uses a function having the following properties to determine the updated key: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key" (see Claim 1-emphasis added), and "said key server using a function having the following properties to determine the updated key: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key" (see Claim 43-emphasis added), which clearly do not simply "express properties that result from the determining step" (emphasis added), as suggested by the Examiner.

Additionally, in the Office Action mailed 12/17/2007, the Examiner has argued that "the Applicant never states that the properties are not for the collusion resistance and

merely argues that the reference is not as specific as the claim language." The Examiner has further argued that "[t]his amounts to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references, especially since the applicant never says that the properties are not for collusion resistance."

Applicant respectfully disagrees and again asserts that for at least the reasons noted above, Balenson does not suggest, and especially does not rise to the level of specificity of, applicant's claim language, namely that "knowledge of said updated first key does not give knowledge of said first key or said second key…and…knowledge of said first key and said updated first key does not give any knowledge of said second key" (emphasis added), as specifically claimed.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to dependent Claims 14 and 15 et al., the Examiner has relied on Page 115, Figure 29 to make a prior art showing of applicant's claimed technique "wherein only said second user is evicted" (see Claim 14 et al.) and "wherein said second user and one or more other users in said set of users are evicted" (see Claim 15 et al.).

Applicant respectfully notes that the above reference excerpt relied on by the Examiner merely discloses the "Blinded ancestral sibling nodes of a CAT." However, nowhere in the above reference excerpt is a technique taught "wherein only said second user is evicted" (see Claim 14 et al. – emphasis added) or "wherein said second user and one or more other users in said set of users are evicted" (see Claim 14 et al. - emphasis added), as claimed by applicant.

Additionally, with respect to dependent Claim 18 et al., the Examiner has relied on Page 10, Figure 2 to make a prior art showing of applicant's claimed technique "wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function."

Applicant respectfully notes that the above reference excerpt relied on by the Examiner merely discloses "[a] one-way function tree for establishing a group key for 8 members." However, merely disclosing a one-way function tree for establishing a group key does not teach a technique "wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function" (emphasis added), as specifically claimed by applicant.

Additionally, with respect to dependent Claims 19 and 48, the Examiner has relied on Page 10, Figure 2 to make a prior art showing of applicant's claimed technique "wherein said determining uses only said first key and said second key" (see the same or similar, but not necessarily identical language in the aforementioned claims). More specifically, the Examiner has argued that "binary trees only account for two child nodes."

Applicant disagrees and again respectfully notes that the above reference excerpt relied on by the Examiner merely discloses "[a] one-way function tree for establishing a group key for 8 members." However, merely disclosing a one-way function tree for establishing a group key does not teach a technique "wherein said determining [an updated first key] uses only said first key and said second key" (emphasis added), in the context specifically claimed by applicant (see independent claims for context).

Furthermore, with respect to dependent Claim 42, applicant respectfully points out that the Examiner has failed to provide a specific prior art rejection of applicant's claimed technique "wherein said subgroup is a self-repairing group, each member of said subgroup capable of independently updating said first key, where said self-repairing uses a reusable power set, said reusable power set using a power set of said members as a basis for group key updates and including 2^N sets, where N includes the number of said members." Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.